Anhang 1 – Technische und organisatorische Maßnahmen zur Datensicherheit gemäß Art. 32 DSGVO

Diese Anlage konkretisiert die gemäß Art. 32 Abs. 1 Datenschutzgrundverordnung (DSGVO) getroffenen technischen und organisatorischen Schutzmaßnahmen unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Bei den nachfolgend dargestellten Schutzmaßnahmen ist folgendes zu berücksichtigen:
Unsere Dienstleistungen erfolgen ohne die Speicherung personenbezogener Daten auf eigenen Serverstrukturen. Der Zugriff auf diese Systeme erfolgt ausschließlich durch gezielte Freigabe von Rechten und Rollen innerhalb der Smart Healthcare Solutions GmbH Organisation. Nachfolgend stellen wir daher nur die von uns getroffenen Maßnahmen zur Zugangskontrolle, Benutzerkontrolle, Übertragungskontrolle, Eingabekontrolle sowie zum Datenschutz-Management dar. Maßnahmen zur lokalen Pseudonymisierung und Verschlüsselung, zum Backup sowie zur Verfügbarkeit und Belastbarkeit entziehen sich unseres Machtbereichs, da die Daten unserer Kunden zu keinem Zeitpunkt bei uns vor Ort lokal gespeichert werden.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
Die Zutrittskontrolle ist durch den Einsatz von Gebäude- und Raumsicherungssystemen, unter anderem einem Zutrittskontrollsysteme durch personalisierte Ausgabe von Schlüsseln gewährleistet. Server, Telekommunikationsanlagen, Netzwerktechnik und ähnliche Anlagen sind in verschließbaren Serverschränken geschützt. Darüber hinaus ist die Zutrittskontrolle durch organisatorische Maßnahmen (z.B. Dienstanweisung, die das Verschließen der Diensträume bei Abwesenheit vorsieht) sichergestellt.

1.2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.
Alle eingesetzten, technischen Systeme verfügen eine Benutzerkennung mit Passwort für Betriebssysteme und eingesetzte Softwareprodukte, inklusive Zweifaktorauthentifizierung soweit verfügbar. Darüber hinaus wurden organisatorische Maßnahmen ergriffen, um unbefugte Einsichtnahmen zu verhindern (z.B. Vorgaben zur Aufstellung von Bildschirmen, Herausgabe von Richtlinien für die Anwender zur Wahl eines „sicheren" Passworts).

1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
Die Zugriffskontrolle wird dadurch gewährleistet, dass geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen, umfassend für alle Systeme etabliert sind. Dabei wurde sowohl eine Differenzierung auf den Inhalt der Daten vorgenommen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten definiert und implementiert, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses).

1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.
Es findet keine Datenaggregation über die verschiedenen datenverarbeitenden Systeme statt. Die Trennung wird auf organisatorischer und physischer Ebene sichergestellt.

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 DSGVO)

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.
Soweit möglich werden die Daten pseudonymisiert in den Systemen mit Hilfe von Kunden IDs oder anderen Referenzidentifikatoren verarbeitet. Eine vollständige Pseudonymisierung ist aufgrund der Dokumentationspflicht der absolvierten e-Kurse mit Zertifikatsausgabe nicht möglich.

2. Integrität (Art. 32 Abs. 1 lit b. DSGVO)

2.1. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
Zur Gewährleistung der Vertraulichkeit bei der elektronischen Datenübertragung werden Verschlüsselungstechniken bei der Übermittlung von Daten eingesetzt. Ein Datenträgertransport bzw. anderweitige Datenweitergabe existieren nicht, da keine Speicherung der Daten außerhalb der technischen Systeme stattfindet.

2.2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.
Die Eingabekontrolle wird durch die Protokollierungen der Aktivitäten und Eingaben in den jeweiligen Systemen erreicht. Die Protokolldaten können durch den Administrator eingesehen und kontrolliert werden. Die Aufbewahrungsfrist der Protokolle richtet sich nach den gesetzlichen Vorgaben.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Da unsere Daten ausschließlich dezentral im Rahmen einer Cloudlösung gespeichert und verwaltet werden, ist eine zufällige Zerstörung oder ein Verlust faktisch ausgeschlossen. Die Service Level Vereinbarungen sichern eine maximale Verfügbarkeit der Daten und Redundanz der Absicherung vor Datenverlust vor.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluation (Art. 32 Abs. 1 lit. d; Art. 25 DSGVO)

Alle Maßnahmen und Datenschutzbestimmungen werden vierteljährig mit der Unterstützung von externen Datenschutzbeauftragen evaluiert und ggf. Aktualisierungen und Anpassungen definiert und implementiert.